APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/825,913	04/16/2004	Jian Zhang	CN920030004US1	8907

36380   7590   05/23/2007
RICHARD M. GOLDMAN
371 ELAN VILLAGE LANE
SUITE 208, CA 95134

EXAMINER
LAFORGIA, CHRISTIAN A

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
05/23/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Office Action Summary	**Application No.**	**Applicant(s)**
		10/825,913	ZHANG ET AL.
		Examiner	**Art Unit**
		Christian La Forgia	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 April 2004*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some *   c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4/16/04*.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1-27 have been presented for examination.

Priority

2.   Acknowledgment is made of applicant's claim for foreign priority under 35

U.S.C. 119(a)-(d).

Information Disclosure Statement

3.   The information disclosure statement (IDS) submitted on 16 April 2004 is in compliance

with the provisions of 37 CFR 1.97. Accordingly, the examiner has considered the information

disclosure statement.

Claim Objections

4.   Claim 11 is objected to because of the following informalities. Claim 11 reads

"computing different keys from different keys having the same father node." For the sake of

examination the examiner shall interpret the claim to be "computing different keys for different

nodes having the same father node." Appropriate correction is required.

Claim Rejections - 35 USC § 101

5.   35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or
> any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and
> requirements of this title.

6.   Claims 20-27 are rejected under 35 U.S.C. 101 because the claimed invention is directed

to non-statutory subject matter. Page 16, lines 14-17 define the claimed media that the program

product is embodied on as "transmission media such as digital and/or analog communications

links, which may be electrical, optical, and/or wireless." The Office's current position is that

claims involving signals encoded with functional descriptive material do not fall within any of

the categories of patentable subject matter set forth in 35 U.S.C. § 101, and such claims are

therefore ineligible for patent protection. *See* 1300 OG 142 (November 22, 2005) (in particular,

see Annex IV(c)).

Claim Rejections - 35 USC § 103

7.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

8.   Claims 1-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent

Application Publication No. 2003/0081792 to Nakano et al., hereinafter Nakano, in view of U.S.

Patent No. 7,095,850 to McGrew, hereinafter McGrew.

9.   As per claims 1 and 20, Nakano teaches a method and a program product for generating

hierarchical keys of digital assets, comprising the steps of:

arranging the digital assets as at least one tree structure, a root node of the tree structure

representing a complete set of the digital assets, other group nodes representing sub-sets in each

level of the digital assets respectively, and the nodes in the lowest level being leaf nodes (Figures

3-5, 18-20, 28, 36, 37, 49, paragraphs 0104-0106, 0302-0307, paragraph 0417-0433);

generating the key of the root node (Figures 2 [block 107], 3 [root – key A], 13 [step

S223], 20 [root – key A], paragraphs 0030, 0032, 0171-0182, 0248); and

starting with the key of the root node, computing level by level the keys of its child nodes

through to leaf nodes (paragraphs 0030, 0032, 0248).

10.   Nakano does not teach using the key of a father node to compute the child node's keys.

11.   McGrew teaches calculating keys from the root to the leaves using a distinct one-way function for each node (column 12, lines 14-23).

12.   It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the key of the father node to compute the key of the child node, since McGrew states at column 5, lines 43-48 that the key updating method can efficiently generate one or more keys that are applicable to ciphers that are used in multicast and group settings.

13.   Regarding claims 2, 11, 16, 19, and 21, Nakano teaches computing different keys for two nodes having the same father node (Figures 3, 4, [node 0 – key B; node 1 – key C; etc.], paragraphs 0030, 0032, 0248).

14.   Regarding claims 3 and 22, Nakano teaches computing different keys for child nodes having the same father node (Figures 3, 4, [node 0 – key B; node 1 – key C; etc.], paragraphs 0030, 0032, 0248).

15.   Regarding claims 4 and 23, Nakano teaches randomly generating the key of the root node (Figures 2 [block 107], 3 [root – key A], 13 [step S223], 20 [root – key A], paragraphs 0030, 0032, 0171-0182, 0248).

16.   Regarding claims 5 and 24, Nakano teaches encrypting corresponding digital assets by using the computed node keys (Figures 8 [block 304], 9 [block 500c], paragraphs 0095, 0209).

17.   With respect to claims 6, 12, and 25, Nakano teaches encrypting the corresponding digital

assets using at least a part of the generated node keys or their deformation (Figures 8 [block

304], 9 [block 500c], paragraphs 0095, 0209).

18.   Concerning claims 7, 13, and 26, Nakano teaches encrypting the digital assets using a

cipher (paragraphs 0011, 0178, 0210), and

        encrypting the cipher using at least a part of the generated node keys or their deformation,

said deformation indicating the result computed from the node keys (Figures 8 [block 304], 9

[block 500c], paragraphs 0095, 0209).

19.   Regarding claims 8 and 27, Nakano teaches wherein the digital assets are chosen from

the group consisting of video, audio and text materials (paragraphs 0207, 0221, 0535, 0607).

20.   As per claim 9, Nakano teaches an apparatus and a server for generating hierarchical keys

of digital assets, comprising:

        a key tree management unit (Figures 1 and 2 [block 100]) for arranging the digital assets

as at least one tree structure for management, a root node of the tree structure representing the

complete set of the digital assets, other group nodes representing sub-sets in each level of the

digital assets respectively, and the nodes in the lowest level being leaf nodes (Figures 3-5, 18-20,

28, 36, 37, 49, paragraphs 0104-0106, 0302-0307, paragraph 0417-0433), said apparatus further

comprises:

a root node key generating unit (Figure 2 [block 107]) for generating the key of the root

node (Figures 3 [root – key A], 13 [step S223], 20 [root – key A], paragraphs 0030, 0032, 0171-

0182, 0248); and

a computing unit for starting with the key of the root node, computing level by level the

keys of its child nodes according to a predetermined function, through to leaf nodes (paragraphs

0030, 0032, 0248).

21.   Nakano does not teach using the key of a father node to compute the child node's keys.

22.   McGrew teaches calculating keys from the root to the leaves using a distinct one-way

function for each node (column 12, lines 14-23).

23.   It would have been obvious to one of ordinary skill in the art at the time the invention

was made to use the key of the father node to compute the key of the child node, since McGrew

states at column 5, lines 43-48 that the key updating method can efficiently generate one or more

keys that are applicable to ciphers that are used in multicast and group settings.

24.   Regarding claims 10, 15, and 18, McGrew teaches computing the keys of the child node

using a one-way function (column 12, lines 14-23).

25.   As per claim 14, Nakano teaches a server apparatus for managing hierarchical keys of

digital assets, comprising:

a key tree management unit (Figures 1 and 2 [block 100]) for arranging the digital assets

as at least one tree structure, a root node of the tree structure representing the complete set of the

digital assets, other group nodes representing sub-sets in each level of the digital assets

respectively, and the nodes in the lowest level being leaf nodes (Figures 3-5, 18-20, 28, 36, 37,

49, paragraphs 0104-0106, 0302-0307, paragraph 0417-0433), said server apparatus further

comprises:

a root node key generating unit (Figure 2 [block 107]) for generating the key of the root

node (Figures 3 [root – key A], 13 [step S223], 20 [root – key A], paragraphs 0030, 0032, 0171-

0182, 0248);

a first computing unit for starting with the key of the root node, computing level by level

the keys of its child nodes through to leaf nodes (paragraphs 0030, 0032, 0248); and

an encrypting unit (Figure 8 [block 304]) for encrypting corresponding digital assets by

using directly or indirectly the computed node keys (Figure 9 [block 500c], paragraphs 0095,

0209).

26.   Nakano does not teach using the key of a father node to compute the child node's keys.

27.   McGrew teaches calculating keys from the root to the leaves using a distinct one-way

function for each node (column 12, lines 14-23).

28.   It would have been obvious to one of ordinary skill in the art at the time the invention

was made to use the key of the father node to compute the key of the child node, since McGrew

states at column 5, lines 43-48 that the key updating method can efficiently generate one or more

keys that are applicable to ciphers that are used in multicast and group settings.

29.   As per claim 17, Nakano teaches a client apparatus for utilizing hierarchical keys of

digital assets, wherein the digital assets being arranged as at least one tree structure, a root node

of the tree structure representing the complete set of the digital assets, other group nodes

representing sub-sets in each level of the digital assets respectively, and the nodes in the lowest

level being leaf nodes, said client apparatus comprises:

a decrypting unit (Figure 9 [blocks 403, 404]) for decrypting the digital assets contained

in all nodes by using the computed keys of all nodes (paragraphs 0218, 0219).

30.   Nakano does not teach a second computing unit for, based on a node key received from a

server apparatus, computing the keys of the nodes in lower levels of said node through to leaf

nodes in turn.

31.   McGrew teaches calculating keys from the root to the leaves using a distinct one-way

function for each node (column 12, lines 14-23).

32.   It would have been obvious to one of ordinary skill in the art at the time the invention

was made to have a second computing unit for, based on a node key received from a server

apparatus, computing the keys of the nodes in lower levels of said node through to leaf nodes in

turn, since McGrew states at column 5, lines 43-48 that the key updating method can efficiently

generate one or more keys that are applicable to ciphers that are used in multicast and group

settings.

Conclusion

33.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure.

34.   The following patents are cited to further show the state of the art with respect to digital

works protected using a key hierarchy, such as:

United States Patent Application Publication No. 2004/0091103 to Martin et al., which is

cited to show transmitting data in which keys are distributed in a binary tree.

United States Patent No. 6,895,503 to Tadayon et al., which is cited to show hierarchical assignment of rights to digital works.

United States Patent Application Publication No. 2003/0204515 to Shadmon et al., which is cited to show a method of indexing data in a hierarchical manner.

United States Patent Application Publication No. 2003/0159037 to Taki et al., which is cited to show digital rights management using keys distributed in a hierarchical tree.

United States Patent Application Publication No. 2003/0161474 to Matsuzaki, which is cited to show group management of distributed data that employs a flexible and unique tree structure.

United States Patent No. 7,103,185 to Srivastava, which is cited to show distributing and updating keys distributed in logical trees.
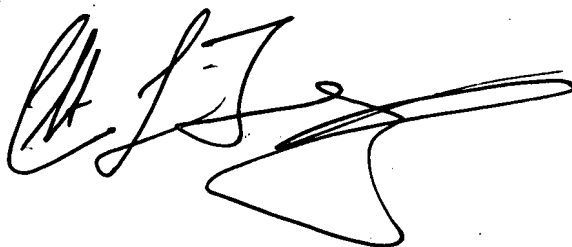
35.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

36.   If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

37.   Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR ·

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

Clf